БАТЛАВ.
УЛСЫН ИХ ХУРЛЫН ГИШҮҮН **Ч.АНАР**

КИБЕР СӨРӨН ТЭСВЭРЛЭХ ТУХАЙ
ХУУЛИЙН ТӨСЛИЙН ҮЗЭЛ БАРИМТЛАЛ

Нэг. Хуулийн төсөл боловсруулах болсон үндэслэл, шаардлага

Монгол Улсад кибер аюулгүй байдлыг хангах тусгайлсан эрх зүйн суурь орчин Кибер аюулгүй байдлын тухай хууль батлагдсанаар бүрдсэн. Гэвч тус хуулийн хэрэгжилтийн явцад байгууллага хоорондын чиг үүргийн зааг, мэдээлэл солилцох дараалал, кибер халдлага, зөрчилд хариу арга хэмжээ авах процесс, аудит болон эрсдэлийн үнэлгээний дараах хяналт, хүний нөөц, санхүүжилт, өгөгдөл хамгааллын уялдаа хангалттай нарийвчлагдаагүй нь тогтоогдсон байна.

Кибер аюулгүй байдлын үндэсний стратегид эрх зүйн орчин, удирдлагын тогтолцоог бэхжүүлэх, онц чухал мэдээллийн дэд бүтцийг хамгаалах, хүний нөөцийн чадавхыг нэмэгдүүлэх, хамтын ажиллагааг өргөжүүлэх, халдлагад хариу үйлдэл үзүүлэх чадавхыг бүрдүүлэх зорилтыг тогтоосон. Стратегийн дараагийн үе шатанд эдгээр зорилтыг хэрэгжүүлэхийн тулд одоогийн хуулийн зохицуулалтыг “кибер аюулгүй байдал”-ын ерөнхий хамгаалалтын хүрээнээс “кибер сөрөн тэсвэрлэх чадавх”-ын тасралтгүй ажиллагаа, урьдчилан сэргийлэх, хариу арга хэмжээ авах, нөхөн сэргээх зохицуулалт руу шинэчлэх шаардлагатай байна.

Хэрэгжилтийн үр дагаврын үнэлгээ, тандан судалгаа, стресс тест болон холбогдох байгууллагуудаас ирүүлсэн саналын дүгнэлтээр кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, ангилах, шилжүүлэх, үндсэн хариуцагчийг тогтоох, явцын мэдээлэл өгөх, бүртгэл хаах, халдлагын дараах дүн шинжилгээ хийх ажиллагаа хуулийн түвшинд тодорхой бус байна. Үүнээс мэдээллийн урсгал тасалдах, хугацаа алдах, давхар мэдэгдэх, хариуцлага тодорхойгүй үлдэх эрсдэл үүсэж байна.

Мөн онц чухал мэдээллийн дэд бүтэцтэй байгууллагын хамрах хүрээг зөвхөн жагсаалтаар тогтоох нь өгөгдлийн ач холбогдол, үйлчилгээ тасалдах бодит хор уршиг, хувийн мэдээлэл боловсруулах цар хүрээ, үүлэн үйлчилгээ, дата төв, программ хангамж, нийлүүлэлтийн сүлжээний хамаарлыг бүрэн тусгахгүй байна. Иймд онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийг эрсдэлд суурилсан шалгуураар ангилж, ялгамжтай үүрэг, хяналт, тайлагналын тогтолцоог хуульчлах шаардлагатай.

Кибер халдлага, зөрчлийн үед техникийн бүртгэлийн мэдээлэл, хортой урсгалтай холбоотой холболтын мэдээлэл, төхөөрөмжийн дүрс хуулбар, халдлагын үзүүлэлт, хэрэглэгчийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцад хамаарах мэдээлэл боловсруулагдах боломжтой. Ийм мэдээллийг боловсруулах, дамжуулах, хадгалах, ашиглах, устгах ажиллагааг хүний хувийн мэдээлэл хамгаалах, төрийн болон албаны нууц хамгаалах, гэмт хэрэг, зөрчил шалган шийдвэрлэх ажиллагаатай уялдуулах эрх зүйн шаардлага байна.

Хоёр. Хуулийн төслийн зорилго, ерөнхий бүтэц, зохицуулах харилцаа, хамрах хүрээ

Хуулийн төслийг “Кибер сөрөн тэсвэрлэх тухай” хуулийн төсөл хэлбэрээр боловсруулна. Хуулийн зорилго нь Монгол Улсын кибер сөрөн тэсвэрлэх чадавхийг хангах, онц чухал болон чухал үйлчилгээний тасралтгүй, найдвартай ажиллагааг хамгаалах, кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах, нөхөн сэргээхтэй холбогдсон харилцааг зохицуулахад оршино.

Хуулийн төсөл нь нийтлэг үндэслэл, кибер сөрөн тэсвэрлэх чадавхийг хангах тогтолцоо, удирдлага, чиг үүрэг, кибер халдлага, зөрчилтэй тэмцэх тогтолцоо, Кибер командлал, мэдээллийн дэд бүтэцтэй этгээдийн ангилал, бүртгэл, үүрэг, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, дотоод удирдлага ба суурь шаардлага, кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, шилжүүлэх, хариу арга хэмжээ авах, кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит, нийлүүлэлтийн сүлжээ, үүлэн үйлчилгээ, программ хангамжийн аюулгүй байдал, эмзэг байдлын удирдлага, мэдээлэл солилцоо, нууцлал, хүний эрх, кибер хямралын удирдлага, хяналт шалгалт, хариуцлага, санхүүжилт, хүний нөөц, сургалт, шилжилтийн зохицуулалт гэсэн бүтэцтэй байна.

Хуулийн төсөлд төрийн байгууллага, онц чухал мэдээллийн дэд бүтэцтэй этгээд, чухал мэдээллийн дэд бүтэцтэй этгээд, төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллага, мэдээллийн систем, сүлжээ, дэд бүтэц ашиглаж, эзэмшиж, эсхүл хариуцаж байгаа хүн, хуулийн этгээд, үүлэн үйлчилгээ, дата төв, домэйн нэр, хостинг, программ хангамж, тоног төхөөрөмжийн үйлчилгээ үзүүлэгч, аудит, эрсдэлийн үнэлгээ хийх этгээд, салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийг хамруулна.

Хуулийн төсөлд кибер халдлага, зөрчлийг нэг цонхны цахим системээр мэдээлэх, бүртгэх, ангилах, шилжүүлэх, буцаан мэдээлэх, бүртгэл хаах, халдлагын дараах дүн шинжилгээ хийх ажиллагааг нарийвчилна. Мөн үйлчилгээ үзүүлэгчийн шуурхай хамтын ажиллагаа, нотлох баримтын бүрэн бүтэн байдал, хортой урсгал, домэйн нэр, хостинг, үүлэн үйлчилгээний ашиглалтыг хязгаарлах нөхцөл, олон нийтэд мэдээлэх дэглэмийг тогтооно.

Аудит, эрсдэлийн үнэлгээний хүрээнд мэргэжлийн шаардлага, хараат бус байдал, ашиг сонирхлын зөрчил, тайлангийн доод агуулга, зөвлөмжийн эрэмбэ, гомдол, мэдээлэл хянан шийдвэрлэх, бүртгэх, бүртгэлийг түдгэлзүүлэх, бүртгэлээс хасах үндэслэлийг тусгана. Нийлүүлэлтийн сүлжээний хүрээнд шинэ мэдээллийн систем, үйлчилгээ нэвтрүүлэхийн өмнөх кибер эрсдэлийн үнэлгээ болон кибер сөрөн тэсвэрлэх чадавхийн аудит, программ хангамж, үүлэн үйлчилгээ, дата төв, туслан гүйцэтгэгчийн эрсдэлийн шаардлагыг зохицуулна.

Хуулийн төсөл эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаа, зөрчил шалган шийдвэрлэх ажиллагаа, тагнуулын ажиллагаа, гүйцэтгэх ажил, төрийн болон албаны нууц хамгаалах нарийвчилсан журмыг давхардуулан зохицуулахгүй. Харин кибер халдлага, зөрчил гэмт хэрэг, зөрчлийн шинжтэй тохиолдолд техникийн хариу арга хэмжээ, нотлох баримт хадгалах ажиллагааг холбогдох хуульд заасан бүрэн эрх, журмын дагуу уялдуулна.

Гурав. Хуулийн төсөл батлагдсаны дараа үүсэх нийгэм, эдийн засаг, хууль зүйн үр дагавар, хүрэх үр дүн, авах арга хэмжээ

Хуулийн төсөл батлагдсанаар төрийн цахим үйлчилгээ, санхүү, эрчим хүч, харилцаа холбоо, эрүүл мэнд, дата төв, төрийн мэдээллийн сан, онц чухал болон чухал үйлчилгээний тасралтгүй, найдвартай ажиллагааг хамгаалах эрх зүйн орчин тодорхой болно. Кибер халдлага, зөрчлийн үед мэдээлэл хүлээн авах, ангилах, шилжүүлэх, хариу арга хэмжээ авах, сэргээн ажиллуулах дараалал нэг мөр болж, иргэн, хуулийн этгээдийн үйлчилгээ тасалдах, хувийн мэдээлэл алдагдах, санхүүгийн болон шууд бус хохирол амсах эрсдэлийг бууруулах нөхцөл бүрдэнэ.

Хүний эрхийн хувьд кибер халдлага, зөрчлийн үед боловсруулагдах хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээллийг зорилгоор хязгаарлах, шаардлагатай хамгийн бага хэмжээнд боловсруулах, хадгалалтын хугацаа тогтоох, хандалтын бүртгэл хөтлөх, дахин ашиглах болон гуравдагч этгээдэд дамжуулах хязгаарыг тогтоох баталгаа бүрдэнэ. Үүний зэрэгцээ хуулийг үзэл бодлоо илэрхийлэх, хууль

ёсны судалгаа хийх, программ хангамж хөгжүүлэх эрхийг үндэслэлгүйгээр хязгаарлах хэрэгсэл болгохгүй байх зарчим хадгалагдана.

Эдийн засгийн хувьд төрийн байгууллага, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдэд аудит, эрсдэлийн үнэлгээ, хамгаалалтын шийдэл, техникийн бүртгэлийн мэдээлэл, нөөцлөлт, сэргээн ажиллуулах орчин, сургалт, хүний нөөцтэй холбоотой нэмэлт зардал үүснэ. Гэвч эдгээр зардал нь кибер халдлага, үйлчилгээ тасалдах, өгөгдөл алдагдах, нөхөн сэргээх ажиллагаа удаашрах, олон нийтийн итгэлцэл алдагдах эрсдэлийг бууруулах урьдчилан сэргийлэх хөрөнгө оруулалтын шинжтэй байна.

Хууль зүйн хувьд байгууллагын чиг үүргийн давхардал, мэдээлэл хүргүүлэх дараллын тодорхойгүй байдал, техникийн хариу арга хэмжээ болон хууль сахиулах ажиллагааны уялдаа, хувийн мэдээлэл болон нууцын хамгаалалтын зааг, аудит ба эрсдэлийн үнэлгээний чанарын хяналт, нэг цонхны цахим систем, салбарын мэдээлэл солилцоо, үүлэн үйлчилгээ, нийлүүлэлтийн сүлжээ, Кибер командлалын ажиллагаатай холбоотой зохицуулалт тодорхой болно.

Хуулийг хэрэгжүүлэхэд жижиг, дунд хуулийн этгээдийн нэмэлт ачаалал, аудит болон эрсдэлийн үнэлгээний зах зээлийн хүчин чадал, төрийн байгууллагын хүний нөөц, санхүүжилт, мэдээллийн нууцлал ба ил тод байдлын тэнцвэр, Кибер аюулгүй байдлын үндэсний төв болон бусад байгууллагын чиг үүргийн заагтай холбоотой эрсдэл үүсэж болно. Эдгээрийг эрсдэлийн түвшинд суурилсан ялгамжтай үүрэг, шилжилтийн хугацаа, арга зүйн дэмжлэг, сургалт, төсвийн төлөвлөлт, хяналт-шинжилгээний механизмаар бууруулна.

Хуулийн төсөл хэрэгжсэнээр кибер халдлага, зөрчлийн мэдээллийн урсгал стандартчилагдах, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийн үүрэг тодорхой болох, аудит, эрсдэлийн үнэлгээний зөвлөмж бодитоор хэрэгжих, өгөгдөл хамгааллын баталгаа сайжрах, салбарын мэдээлэл солилцоо идэвхжих, кибер хямралын үед төр, хувийн хэвшлийн шуурхай зохион байгуулалт бүрдэх үр дүнд хүрнэ.

Дөрөв. Хуулийн төсөл нь Үндсэн хууль, олон улсын гэрээ, бусад хуультай уялдах байдал, дагалдан боловсруулах хуулийн санал

Хуулийн төслийг Монгол Улсын Үндсэн хууль, Монгол Улсын нэгдэн орсон олон улсын гэрээ, олон улсын эрх зүйн нийтээр хүлээн зөвшөөрсөн зарчим, хэм хэмжээ болон үндэсний аюулгүй байдлын бодлоготой нийцүүлэн боловсруулна. Хуулийн төсөл нь үндэсний аюулгүй байдал, нийтийн ашиг сонирхлыг хамгаалах зорилготой боловч хүний эрх, эрх чөлөө, хувийн мэдээлэл хамгаалах баталгаа, хууль ёсны судалгаа, программ хангамж хөгжүүлэх, мэдээлэл авах эрхийг үндэслэлгүйгээр хязгаарлахгүй байх зарчимд тулгуурлана.

Хүний хувийн мэдээлэл хамгаалах тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Төрийн болон албаны нууцын тухай хуультай уялдуулах хүрээнд кибер халдлага, зөрчлийн үед дамжуулах техникийн бүртгэлийн мэдээлэл, хортой урсгалтай холбоотой холболтын мэдээлэл, шинжилгээний материал, хэрэглэгчийн мэдээлэл, аудитын тайлан, эрсдэлийн үнэлгээ, эмзэг байдлын мэдээллийн нууцлал, хадгалалт, хандалт, нийтэд мэдээлэх болон хязгаарлах нөхцөлийг тодорхой болгоно.

Эрүүгийн хууль, Зөрчлийн тухай хууль, Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль, Зөрчил шалган шийдвэрлэх тухай хууль, Тагнуулын байгууллагын тухай хууль, Батлан хамгаалах тухай хууль, Зэвсэгт хүчний тухай хууль, Гамшгаас хамгаалах тухай хуультай уялдуулах хүрээнд кибер халдлага, зөрчлийн техникийн хариу арга хэмжээ нь гэмт хэрэг, зөрчил шалган шийдвэрлэх ажиллагаа болон үндэсний аюулгүй байдлын бүрэн эрхтэй зөрчилдөхгүй байх зохицуулалтыг тусгана.

Төсвийн тухай хууль болон төрийн болон орон нутгийн өмчийн хөрөнгөөр бараа, ажил, үйлчилгээ худалдан авах ажиллагааны тухай хуультай уялдуулах хүрээнд кибер сөрөн тэсвэрлэх чадавхийг хангах зардлыг төсөв, бизнес төлөвлөгөөнд тусгах, техник, программ хангамж, үүлэн үйлчилгээ, дата төв, кибер аюулгүй байдлын үйлчилгээ худалдан авах гэрээнд аюулгүй байдлын шаардлага, нийлүүлэлтийн дараах үйлчилгээ, эмзэг байдлын мэдээлэл, аудитын мэдээлэл авах эрхийг тусгах шаардлагатай.

Хуулийн төсөлтэй уялдуулан Кибер сөрөн тэсвэрлэх тухай хуулийг батлах, 2021 оны 12 дугаар сарын 17-ны өдөр баталсан Кибер аюулгүй байдлын тухай хуулийг хүчингүй болсонд тооцох асуудлыг дагалдах хуулийн төсөлд тусгана. Мөн дээр дурдсан холбогдох хуулиудад нэр томьёо, байгууллагын чиг үүрэг, мэдээлэл солилцоо, төсөв, худалдан авалтын шаардлага, хариуцлагын зохицуулалтын нэмэлт, өөрчлөлт шаардлагатай эсэхийг тусгайлан нягтална.

Хуулийг хэрэгжүүлэх зорилгоор онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийг ангилах, бүртгэх, жагсаалт тогтоох, кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, ангилах, шилжүүлэх, хариу арга хэмжээ авах, нэг цонхны цахим систем ажиллуулах, аудит, эрсдэлийн үнэлгээ хийх, бүртгэх, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах, үүлэн үйлчилгээ болон нийлүүлэлтийн сүлжээний эрсдэлийн шаардлага тогтоох, төсөв, тайлагнал, хүний нөөц, сургалтын журмыг боловсруулна.

-----oOo-----